Cisco IOS-Passwortverschlüsselung - Fakten

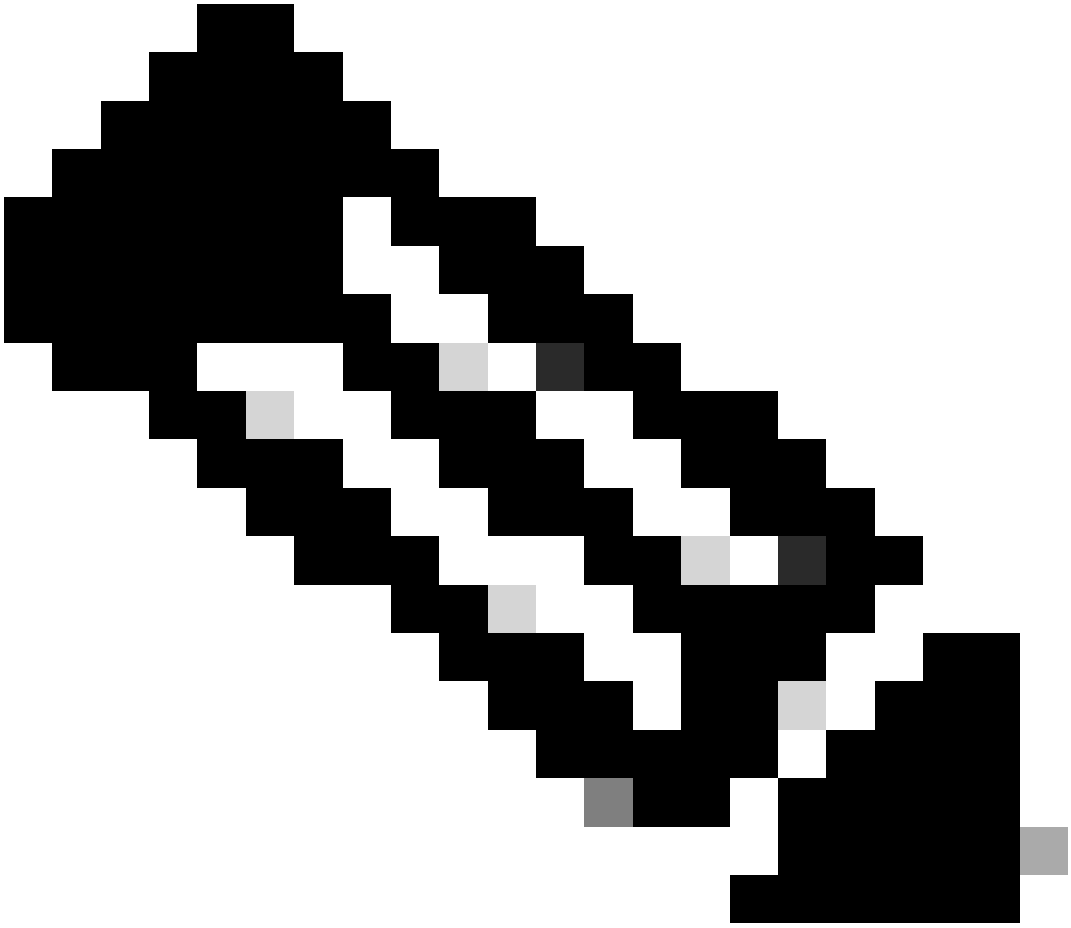
Inhalt

Einleitung

Dieses Dokument beschreibt das Sicherheitsmodell, das der Cisco Passwortverschlüsselung zugrunde liegt, und die Sicherheitseinschränkungen dieser Verschlüsselung.

Hintergrund

Eine nicht von Cisco stammende Quelle hat ein Programm zur Entschlüsselung von Benutzerkennwörtern (und anderen Kennwörtern) in Cisco Konfigurationsdateien veröffentlicht. Das Programm entschlüsselt keine mit dem **enable secret** Befehl festgelegten Kennwörter. Die unerwarteten Bedenken, die dieses Programm bei Cisco-Benutzern ausgelöst hat, haben den Verdacht aufkommen lassen, dass viele Benutzer die Cisco Passwortverschlüsselung für mehr Sicherheit als ursprünglich vorgesehen verwenden.



Hinweis: Cisco empfiehlt, dass alle Cisco IOS®-Geräte das Sicherheitsmodell für Authentifizierung, Autorisierung und Abrechnung (Authentication, Authorization, Accounting - AAA) implementieren. AAA kann lokale, RADIUS- und TACACS+-Datenbanken verwenden.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Benutzerkennwörter

Benutzerkennwörter und die meisten anderen Kennwörter (*nicht* **enable secret**s) in Cisco IOS-Konfigurationsdateien werden mit einem Schema verschlüsselt, das nach modernen kryptografischen Standards sehr schwach ist.

Obwohl Cisco kein Entschlüsselungsprogramm vertreibt, sind mindestens zwei verschiedene Entschlüsselungsprogramme für Cisco IOS-Passwörter im Internet öffentlich zugänglich; die erste öffentliche Veröffentlichung eines solchen Programms, die Cisco bekannt ist, war Anfang 1995. Wir würden erwarten, dass jeder Amateur-Kryptograf in der Lage ist, mit wenig Aufwand ein neues Programm zu erstellen.

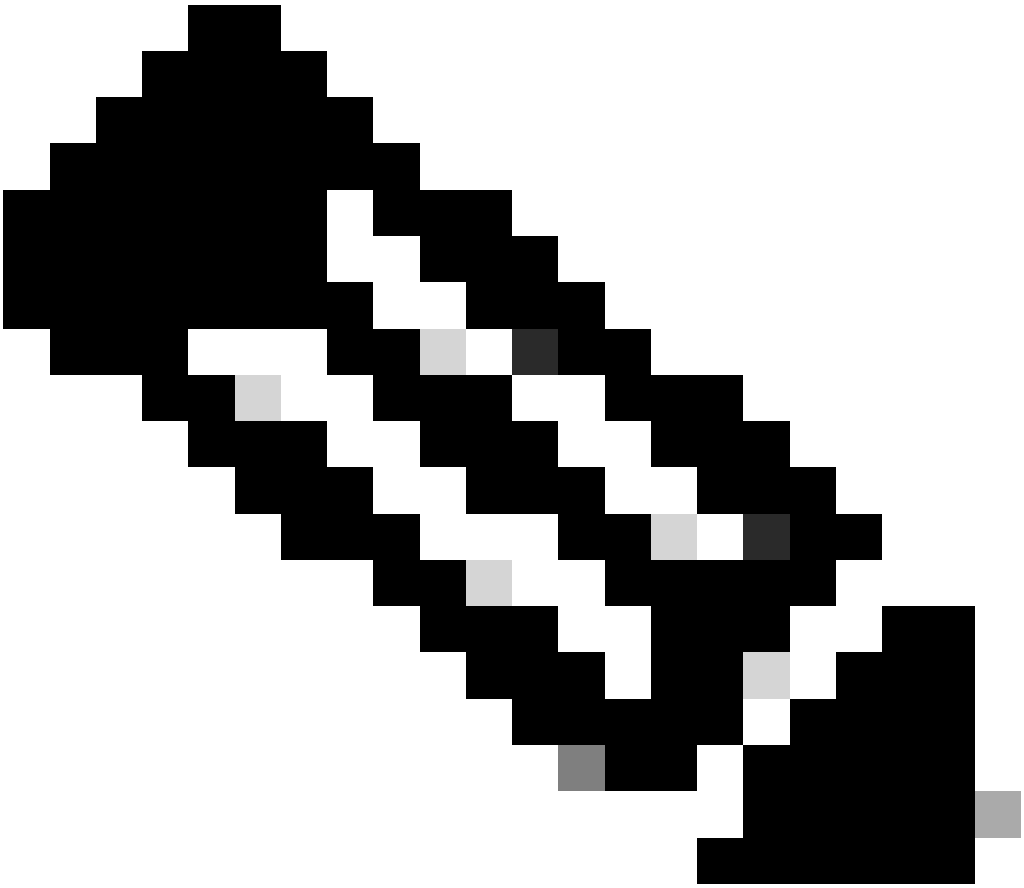
Das von Cisco IOS verwendete Schema für Benutzerkennwörter war nie als Reaktion auf einen zielgerichteten, intelligenten Angriff gedacht. Das Verschlüsselungsschema wurde entwickelt, um Passwortdiebstahl durch einfaches Snooping oder Sniffing zu vermeiden. Sie war nie dazu gedacht, jemanden zu schützen, der versucht, die Passwörter für die Konfigurationsdatei zu knacken.

Aufgrund des schwachen Verschlüsselungsalgorithmus war es immer die Position von Cisco, dass Benutzer jede Konfigurationsdatei, die Kennwörter enthält, als vertrauliche Informationen behandeln, genauso wie eine Klartextliste von Kennwörtern.

Die Befehle enable secret und enable password

Die Verwendung des enable password Befehls wird nicht mehr empfohlen. Verwenden Sie den enable secret Befehl zur Erhöhung der Sicherheit. Der einzige Fall, in dem der **enable password** Befehl getestet werden kann, ist, wenn sich das Gerät in einem Bootmodus befindet, der den enable secret Befehl nicht unterstützt.

Aktiviert Geheimnisse werden mit dem MD5-Algorithmus gehasht. Soweit Cisco weiß, ist es unmöglich, einen Aktivierungsschlüssel basierend auf dem Inhalt einer Konfigurationsdatei wiederherzustellen (außer durch offensichtliche Wörterbuchangriffe).



Hinweis: Dies gilt nur für Kennwörter, die mit enable secret festgelegt wurden, und nicht für Kennwörter, die mit **enable password** festgelegt wurden. Tatsächlich ist die Stärke der verwendeten Verschlüsselung der einzige signifikante Unterschied zwischen den beiden Befehlen.

Welches Cisco IOS-Image unterstützt enable secret?

Überprüfen Sie Ihr Boot-Image mit dem **show version** Befehl Ihres normalen Betriebsmodus (vollständiges Cisco IOS-Image), um festzustellen, ob das Boot-Image den **enable secret** Befehl unterstützt. Wenn ja, entfernen Sie die **enable password**. Wenn das Boot-Image keine Unterstützung bietet, beachten Sie **enable secret**folgende Hinweise:

- Die Verwendung eines Aktivierungskennworts kann sich als unnötig erweisen, wenn Sie über physische Sicherheit verfügen, sodass das Gerät nicht in das Boot-Image geladen werden kann.

- Wenn jemand physischen Zugriff auf das Gerät hat, kann er die Gerätesicherheit ganz einfach untergraben, ohne auf das Boot-Image zugreifen zu müssen.

- Wenn Sie die **enable password** auf den gleichen Wert wie die enable secret eingestellt haben, haben Sie die enable secret so anfällig für Angriff wie die **enable password**.

    - Wenn Sie **enable password** einen anderen Wert festlegen, da das Boot-Image nicht unterstützt wird, **enable secret**müssen sich die Router-Administratoren ein neues Kennwort merken, das selten auf ROMs verwendet wird, die den **enable secret** Befehl nicht unterstützen. Mit einem separaten Aktivierungskennwort müssen sich Administratoren das Kennwort merken, wenn sie einen Ausfall für ein Software-Upgrade erzwingen. Dies ist der einzige Grund, sich im Startmodus anzumelden.

Andere Kennwörter

Fast alle Kennwörter und anderen Authentifizierungszeichenfolgen in Cisco IOS-Konfigurationsdateien werden mit dem schwachen, umkehrbaren Schema verschlüsselt, das für Benutzerkennwörter verwendet wird.

Um festzustellen, welches Schema zum Verschlüsseln eines bestimmten Kennworts verwendet wurde, markieren Sie die Ziffer vor der verschlüsselten Zeichenfolge in der Konfigurationsdatei. Wenn diese Ziffer eine 7 ist, wurde das Kennwort mit dem schwachen Algorithmus verschlüsselt. Wenn die Ziffer eine 5 ist, wurde das Kennwort mit dem stärkeren MD5-Algorithmus gehasht.

Beispiel: Im Konfigurationsbefehl:

<#root>

enable secret 5 1iUjJ$cDZ03KKGh7mHfX2RSbDqP.

Der "enable secret"-Schlüssel wurde mit MD5 gehasht, während im Befehl:

<#root>

username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D

Das Kennwort wurde mit dem schwachen umkehrbaren Algorithmus verschlüsselt.

Konfigurationsdateien

Wenn Sie Konfigurationsinformationen per E-Mail senden, bereinigen Sie die Konfiguration anhand der Kennwörter vom Typ 7. Sie können den show tech-support Befehl verwenden, der die Informationen standardmäßig bereinigt. Eine Beispiel-**show tech-support** Befehlsausgabe ist hier dargestellt:

<#root>

```
...
 hostname routerA
 !
 aaa new-model
 aaa authentication login default local
 aaa authentication ppp default if-needed local
```

enable secret 5 <removed>

```
!


username jdoe password 7 <removed>
username headquarters password 7 <removed>
username hacker password 7 <removed>


...
```

Wenn Sie Ihre Konfigurationsdateien auf einem TFTP-Server (Trivial File Transfer Protocol) speichern, ändern Sie die Berechtigungen für diese Datei, wenn sie nicht verwendet wird, oder stellen Sie sie hinter eine Firewall.

Kann der Algorithmus geändert werden?

Cisco hat keine unmittelbaren Pläne, einen sichereren Verschlüsselungsalgorithmus für Cisco IOS-Benutzerkennwörter zu unterstützen. Wenn Cisco sich entschließt, eine solche Funktion in Zukunft einzuführen, bedeutet dies definitiv einen zusätzlichen Verwaltungsaufwand für die Benutzer, die sich dafür entscheiden, diese Funktion zu nutzen.

Im Allgemeinen ist es nicht möglich, Benutzerkennwörter auf den MD5-basierten Algorithmus umzustellen, der für enable secrets verwendet wird, da MD5 ein unidirektionaler Hash ist und das Kennwort überhaupt nicht aus den verschlüsselten Daten wiederhergestellt werden kann. Um bestimmte Authentifizierungsprotokolle (insbesondere CHAP) zu unterstützen, benötigt das System Zugriff auf den unverschlüsselten Text von Benutzerkennwörtern und muss diese daher mit einem umkehrbaren Algorithmus speichern.

Aufgrund wichtiger Verwaltungsprobleme wäre es keine leichte Aufgabe, auf einen stärker umkehrbaren Algorithmus wie Data Encryption Standard (DES) umzusteigen. Zwar ließe sich Cisco IOS leicht so ändern, dass DES zur Verschlüsselung von Kennwörtern verwendet wird, es bestünde jedoch kein Sicherheitsvorteil, wenn alle Cisco IOS-Systeme denselben DES-Schlüssel verwenden würden. Würden verschiedene Schlüssel von verschiedenen Systemen verwendet, wäre der Verwaltungsaufwand für alle Cisco IOS-Netzwerkadministratoren geringer, und die Übertragbarkeit von Konfigurationsdateien zwischen Systemen würde beeinträchtigt. Die Benutzernachfrage nach einer stärkeren, umkehrbaren Passwortverschlüsselung ist gering.

Zugehörige Informationen

- **Verfahren zur Kennwortwiederherstellung**
- **Cisco Leitfaden zum Absichern von Cisco IOS-Geräten**

- **Technischer Support – Cisco Systems**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.